PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-142110
(43)Date of publication of application : 17.05.2002

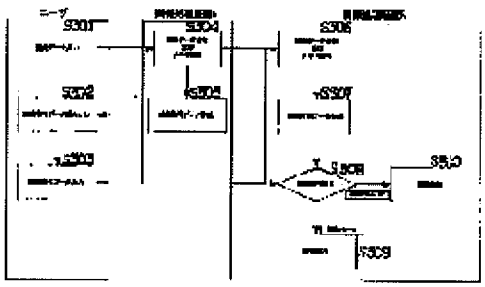
(51)Int.Cl. H04N 1/40
H04N 1/41
// G09C 1/00

(21)Application number : 2000-336103
(22)Date of filing : 02.11.2000

(71)Applicant : RICOH CO LTD
(72)Inventor : NISHIDA TAIRA

(54) IMAGE PROCESSING DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an image processing device which is capable of preventing an authentication code from leaking out and ensuring security.
SOLUTION: When an image data input (S301) is carried out, image data are transmitted to an image processing device B and stored in a memory (S304). Authentication code data are formed for the image data (S305) and stored in a storage medium, and the authentication code is inputted into the image processing device B (S303) when an indication that authentication code is read out is issued (S302). The image processing device B receives image data, stores them in a storage medium (S306), and forms authentication code data (S307). The authentication code is collated (S308), and when it is found that the authentication code is identified, the image is outputted (S309). When the authentication code is not identified, a warning is displayed (S310).



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－142110
（P2002－142110A）
(43)公開日　平成14年５月17日(2002.5.17)

(51)Int.Cl.⁷		識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｎ	1/40		Ｈ０４Ｎ	1/41	Ｚ　５Ｃ０７７
	1/41		Ｇ０９Ｃ	1/00	６４０Ｄ　５Ｃ０７８
// Ｇ０９Ｃ	1/00	６４０	Ｈ０４Ｎ	1/40	Ｚ　５Ｊ１０４

審査請求　未請求　請求項の数３　ＯＬ　（全７頁）

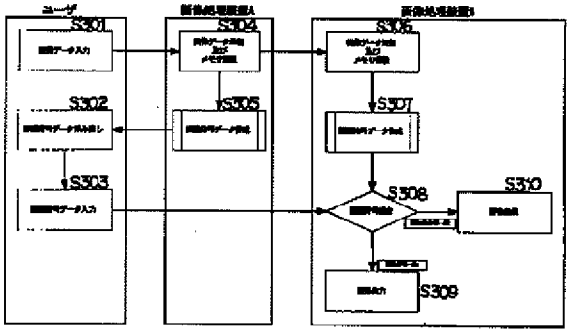
(21)出願番号　特願2000－336103(P2000－336103)
(22)出願日　平成12年11月２日(2000.11.2)

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(72)発明者　西多　平
東京都大田区中馬込１丁目３番６号　株式会社リコー内

Ｆターム(参考)　5C077 LL14 NP07 PP55 PP66 PQ20
RR21 SS05
5C078 BA12 CA01
5J104 AA08 LA05

(54)【発明の名称】　画像処理装置

(57)【要約】
【課題】　認証符号の漏洩を防止し、セキュリティを確保することができる画像処理装置を提供すること。
【解決手段】　画像データ入力（Ｓ３０１）を行うと、画像データの送信およびメモリ蓄積（Ｓ３０４）処理で画像処理装置Ｂに画像データを送信し、メモリに蓄積する。そして、画像データに対して認識符号データ作成（Ｓ３０５）により作成された認証符号を認証符号データ読み出し（Ｓ３０２）の指示があると、が記憶媒体に保存して画像処理装置Ｂに入力する（認証符号データ入力（Ｓ３０３）。画像処理装置Ｂは、画像データに対して画像データ受信およびメモリ蓄積（Ｓ３０６）処理と認証符号データの作成（Ｓ３０７）処理を行う。そして、認証符号照合（Ｓ３０８）処理により、認証符号が一致した場合、画像出力（Ｓ３０９）を行う。不一致の場合、警告表示（Ｓ３１０）を行う。



1

【特許請求の範囲】

【請求項１】　データ圧縮処理して認証符号化データとすることができる他の画像処理装置とネットワークを介して接続可能な画像処理装置において、

前記他の画像処理装置からデータ圧縮処理前のデータを受信するデータ受信手段と、

前記データ受信手段によって受信したデータを画像形成して出力するデータ出力手段と、

前記データ受信手段により受信したデータにデータ圧縮処理を施して認証用データを作成する認証データ作成手段と、

前記他の画像処理装置によってデータ圧縮処理された認証符号化データを別途受領し、この受領した認証符号化データと前記認証データ作成手段によって作成された認証用データとが一致するか判断する比較照合手段と、を備え、

前記比較照合手段によって前記認証符号データと前記認証データとが一致すると判断された場合、前記データ出力手段は該当するデータを画像形成して出力することを特徴とする画像処理装置。

【請求項２】　前記他の画像処理装置によるデータ圧縮処理の回数をネットワークを介して設定する回数設定手段をさらに備えたことを特徴とする請求項２記載の画像処理装置。

【請求項３】　前記他の画像処理装置によってデータ圧縮処理される際のデータサイズをネットワークを介して指定する指定手段をさらに備えたことを特徴とする請求項１または請求項２記載の画像処理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、画像情報のディジタル処理を行い、半導体メモリなどのメモリ技術をにより画像情報の認証を行う画像処理装置に関する。

【０００２】

【従来の技術】近年、ネットワークの発展に伴い、複数の端末装置と画像処理装置とがネットワーク接続され、端末装置からの操作指示やネットワーク接続された他の画像処理装置からの指示により画像データを送受信し、ネットワーク内の他の画像処理装置からも出力することができる画像処理システムが広く利用されている。このような画像処理システムにおいて画像処理装置Ａから他の画像処理装置Ｂへ画像データを転送し、画像処理装置Ｂより画像を出力させる場合、ユーザがいないところで画像が出力されることがある。

【０００３】図７の従来の画像処理システムに示されるように、画像処理装置Ａから画像データが転送されると、画像処理装置Ｂからすぐに画像出力されてしまい、画像処理装置Ａから画像データを転送したユーザが画像処理装置Ｂに出力画像を取りに行くまでに第三者により出力画像を見られたり持ち去られたりするなど、出力画像のセキュリティが確保されないことがある。このような場合に対して従来では、画像処理装置Ａは画像データと合わせてパスワード情報を記載した付帯データも転送し、画像処理装置Ａから画像処理装置Ｂへ画像データを転送しても、画像処理装置Ｂはすぐに画像を出力せずに蓄積しておく。そして、画像処理装置Ｂでは、ユーザが入力したパスワードと画像データと合わせて転送されてきた付帯データ（パスワード情報）に記されている内容とを照合し、一致した場合のみ画像を出力することによるセキュリティ確保が提案されている。ネットワーク接続された画像処理システム間で送受信する画像データのセキュリティ保護のために、画像データ自体にパスワードを付加することにより、画像処理装置での画像データの出力際にはパスワード入力によりユーザの認証が行われていた。

2

【０００４】ところで、特開平７－１８４０６８号公報には、データメモリに記憶される機密ファイルごとにパスワードを付与し、このパスワードが一致した場合に機密ファイルの出力を行うようにした画像処理システムが記載されている。また、特開平９－４６４６８号公報には、端末装置からパスワードおよび文書データを入力し、ディスク装置に装着されたディスクに付されているパスワードと一致する場合にディスクに入力した文書データを記憶格納し、プリンタ部から該当する文書データを出力する画像処理装置が記載されている。

【０００５】

【発明が解決しようとする課題】しかしながら、上述のようなパスワードを付加した画像データをネットワーク内で転送する方法では、パスワード情報（以下、認証符号という）が漏洩してしまう場合がある。認証符号を画像データに付加する際に時間を要したり、また、認証符号を画像データに付加したことによってネットワーク間で送受信されるデータ量が多くなり、データ転送時間を要してしまうことがある。そこで、本発明の第１の目的は、認証符号の漏洩を防止し、ユーザがいないところで画像データが出力されることがないようにセキュリティを確保することができる画像処理装置を提供することである。本発明の第２の目的は、認証符号のデータ量を任意のサイズに削減することができる画像処理装置を提供することである。本発明の第３の目的は、認証符号のデータ量に関わらず、短時間で認証符号のデータを作成することができる画像処理装置を提供することである。

【０００６】

【課題を解決するための手段】請求項１記載の発明では、データ圧縮処理して認証符号化データとすることができる他の画像処理装置とネットワークを介して接続可能な画像処理装置において、前記他の画像処理装置からデータ圧縮処理前のデータを受信するデータ受信手段と、前記データ受信手段によって受信したデータを画像形成して出力するデータ出力手段と、前記データ受信手

段により受信したデータにデータ圧縮処理を施して認証用データを作成する認証データ作成手段と、前記他の画像処理装置によってデータ圧縮処理された認証符号化データを別途受領し、この受領した認証符号化データと前記認証データ作成手段によって作成された認証用データとが一致するか判断する比較照合手段と、を備え、前記比較照合手段によって前記認証符号データと前記認証データとが一致すると判断された場合、前記データ出力手段は該当するデータを画像形成して出力することにより、前記第１の目的を達成する。

【０００７】請求項２記載の発明では、請求項１記載の発明において、前記他の画像処理装置によるデータ圧縮処理の回数をネットワークを介して設定する回数設定手段をさらに備えたことにより、前記第２の目的を達成する。請求項３記載の発明では、請求項１または請求項２記載の発明において、前記他の画像処理装置によってデータ圧縮処理される際のデータサイズをネットワークを介して指定する指定手段をさらに備えたことにより、前記第３の目的を達成する。

【０００８】

【発明の実施の形態】以下、本発明の好適な実施の形態について図１ないし図６を参照して詳細に説明する。図１は、本実施の形態に係る画像処理システムの構成を示した図である。本実施の形態の画像処理装置Ｂは、画像データが転送されるとすぐに画像出力するのではなく、ネットワーク回線上には画像データのみを転送し、ユーザによる画像データの認証を行ってから画像出力するようになっている。画像処理装置Ａにおいて作成された認証符号をユーザが読み出して記憶媒体１に保存する。そして、この記憶媒体を画像処理装置Ｂに入力する。画像処理装置Ｂでは画像データのみをネットワークを介して画像処理装置Ａから受信し、この受信した画像データに対する認証符号を作成する。画像処理装置Ａにおいて作成された認証符号（記憶媒体１に保存された認証符号）と画像処理装置Ｂで作成された認証符号を照合し、認証符号が一致した場合、画像処理装置Ｂは画像出力を行うようになっている。

【０００９】まず、第１の実施形態について説明する。図２は、第１の実施形態の認証符号の作成の方法を示した図である。画像データをデータ圧縮器によって圧縮処理をして認証符号を作成する。データ圧縮器のアルゴリズムは、予め定められたものを利用する。ユーザの確認に利用する認証符号として考えられる最も確実な認証符号は、画像データそのものであるが、画像データはデータ量が大きく扱いにくいので、画像データを圧縮することで認証符号のデータ量を削減することができる、データ圧縮したものは符号化されているので、漏洩した場合にも解読されにくいなどの理由から認証符号作成にデータ圧縮器を利用する。あらかじめ定めたデータ圧縮アルゴリズムとしては、例えば画像処理装置Ａ、Ｂの互換性から標準化されたアルゴリズム、圧縮率を上げるために非可逆のアルゴリズムなどを利用するのが良いが、これに限られるものではない。

【００１０】図３は、第１の実施形態の画像処理装置Ａ、画像処理装置Ｂの動作を示した流れ図である。まず、ユーザが画像処理装置Ａにおいて「画像データ入力（ステップ３０１）」を行うと、画像処理装置Ａによってその入力された画像データを「画像データの送信およびメモリ蓄積（ステップ３０４）」処理の過程で画像処理装置Ｂに画像データを送信すると同時に、受信した画像データを画像処理装置Ａのメモリに蓄積する。画像処理装置Ａでは、メモリに蓄積した画像データに対して図２に示したようなデータ圧縮器によって「認識符号データ作成（ステップ３０５）」を行う。次に、ユーザが画像処理装置Ａから「認証符号データ読み出し（ステップ３０２）」を行うと、「認識符号データ作成（ステップ３０５）」で作成された認証符号が記憶媒体に保存される。そして、ユーザは認証符号が保存された記憶媒体を画像処理装置Ｂに入力する（「認証符号データ入力（ステップ３０３）」）。

【００１１】画像処理装置Ｂは、画像処理装置Ａから受信した画像データに対して「画像データ受信およびメモリ蓄積（ステップ３０６）」の処理を行う。そして、画像処理装置Ａで作成された認証符号と同様にデータ圧縮により「認証符号データの作成（ステップ３０７）」の処理を行う。画像処理装置Ｂで作成された認証符号とユーザが入力した認証符号とを比較照合する「認証符号照合（ステップ３０８）」の処理によって、認証符号が一致するかどうかを判断する。「認証符号照合（ステップ３０８）」の過程で２つの認証符号が完全に一致した場合、「画像出力（ステップ３０９）」を行う。２つの認証符号が不一致の場合、画像出力をしない「警告表示（ステップ３１０）」を行って、例えばアナウンスする、画像処理装置の表示パネルに表示するなどユーザに知らせるようになっている。

【００１２】次に、第２の実施形態について説明する。図４は、第２の実施形態の認証符号の作成方法を示した図である。図４のように認証符号のデータは、１度データ圧縮処理によって作成された画像データをさらにデータ圧縮処理を行うようになっている。すなわち、画像データを再帰的に複数回（以降、Ｎ回とする）データ圧縮処理を行うことによって作成し、認証符号のデータ量を任意の大きさまで削減することができる。図５は、第２の実施形態の画像処理装置Ａ、画像処理装置Ｂの動作を示した流れ図である。まず、ユーザが画像処理装置Ａにおいて「画像データ入力（ステップ４０１）」を行うと、画像処理装置Ａによってその入力された画像データを「画像データの送信およびメモリ蓄積（ステップ４０６）」処理の過程で画像処理装置Ｂに画像データを送信すると同時に、受信した画像データを画像処理装置Ａの

メモリに蓄積する。画像処理装置Ａでは、メモリに蓄積した画像データに対して図２に示したようなデータ圧縮器によって「認識符号データ作成（ステップ４０７）」を行う。

【００１３】ここで、本実施の形態では、「認証符号データの作成（ステップ４０７）」の際、画像データのデータ圧縮処理をＮ回を設定しなくてはいけないので、画像処理装置Ａに対してユーザが「認証符号データ情報入力（ステップ４０２）」の処理を行う。この「認識符号データ作成（ステップ４０７）」を行う前に、ユーザが「認識符号作成情報入力（ステップ４０２）」としてデータ圧縮処理を行うＮ回の入力の基づいて、画像処理装置Ａは「認識符号データ作成（ステップ４０７）」を行う。ユーザが画像処理装置Ａから「認証符号データ読み出し（ステップ４０３）」を行うと、「認識符号データ作成（ステップ４０７）」で作成された認証符号が記憶媒体に保存される。そして、ユーザは認証符号が保存された記憶媒体を画像処理装置Ｂに入力する（「認証符号データ入力（ステップ４０５）」）。

【００１４】画像処理装置Ｂは、画像処理装置Ａから受信した画像データに対して「画像データ受信およびメモリ蓄積（ステップ４０８）」の処理を行う。そして、画像処理装置Ａで作成された認証符号と同様にデータ圧縮により「認証符号データの作成（ステップ４０９）」の処理を行う。ここで、本実施の形態では、「認証符号データの作成（ステップ４０９）」の際、画像処理装置Ａと同様に、画像データのデータ圧縮処理をＮ回を設定しなくてはいけないので、画像処理装置Ｂに対してユーザが「認証符号データ情報入力（ステップ４０４）」の処理を行う。この「認識符号データ作成（ステップ４０９）」を行う前に、ユーザが「認識符号作成情報入力（ステップ４０４）」としてデータ圧縮処理を行うＮ回の入力の基づいて、画像処理装置Ａは「認識符号データ作成（ステップ４０９）」を行う。

【００１５】そして、画像処理装置Ｂで作成された認証符号とユーザが入力した認証符号とを比較照合する「認証符号照合（ステップ４１０）」の処理によって、認証符号が一致するかどうかを判断する。「認証符号照合（ステップ４１０）」の過程で２つの認証符号が完全に一致した場合、「画像出力（ステップ４１１）」を行う。２つの認証符号が不一致の場合、画像出力をしない「警告表示（ステップ４１２）」を行って、例えばアナウンスする、画像処理装置の表示パネルに表示するなどユーザに知らせるようになっている。

【００１６】次に、第３の実施形態について説明する。図６は、第３の実施形態の認証符号の作成方法を示した図である。本実施の形態では、認証符号のデータは、画像データのうちユーザが指定した部分のみデータ圧縮器によってデータ圧縮処理を行って作成される。これにより、認証符号のデータ量を任意の大きさまで短時間で削減することができ、処理速度の短縮を図ることができる。本実施の形態の流れは、図３および図５の流れと同様であるが、図５の「認証符号作成情報入力（ステップ４０２）」において、ユーザが認証符号作成情報として圧縮処理する画像部分を指定する点が第２の実施形態と異なる。なお、各実施の形態において画像処理装置Ａ、Ｂは、パーソナルコンピュータ、複写機、印刷装置、プリンタ装置など画像データ処理を行う装置（ＯＡ機器全般を含む）であればよいとする。

【００１７】

【発明の効果】請求項１記載の発明では、比較照合手段によって認証符号データと認証データとが一致すると判断された場合、データ出力手段は該当するデータを画像形成して出力するので、認証符号の漏洩、第三者に出力画像を見せないなどのセキュリティを確保できる。請求項２記載の発明では、他の画像処理装置によるデータ圧縮処理の回数をネットワークを介して設定する回数設定手段をさらに備えたので、設定されたデータ量まで認証符号の削減ができ、認証符号の漏洩、第三者に出力画像を見せないなどのセキュリティ確保をすることができる。

【００１８】請求項３記載の発明では、他の画像処理装置によってデータ圧縮処理される際のデータサイズをネットワークを介して指定する指定手段をさらに備えたので、設定されたデータ量まで認証符号データを削減することができ、データ圧縮処理の処理速度を短縮することができる。

【図面の簡単な説明】

【図１】本実施の形態に係る画像処理システムの構成を示した図である。

【図２】第１の実施形態の認証符号の作成の方法を示した図である。

【図３】第１の実施形態の画像処理装置Ａ、画像処理装置Ｂの動作を示した流れ図である。

【図４】第２の実施形態の認証符号の作成の方法を示した図である。

【図５】第２の実施形態の画像処理装置Ａ、画像処理装置Ｂの動作を示した流れ図である。

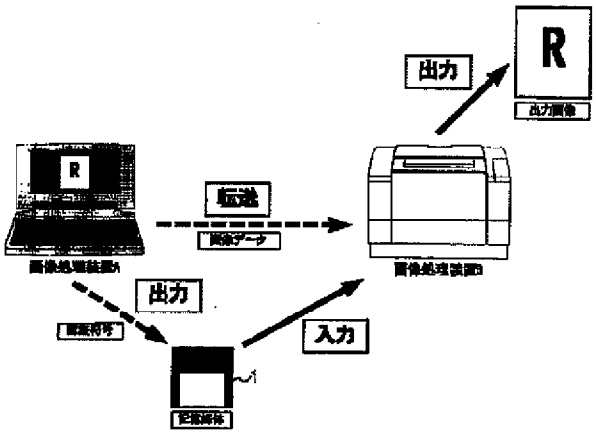
【図６】第３の実施形態の認証符号の作成方法を示した図である。

【図７】従来の画像処理システムを示した図である。

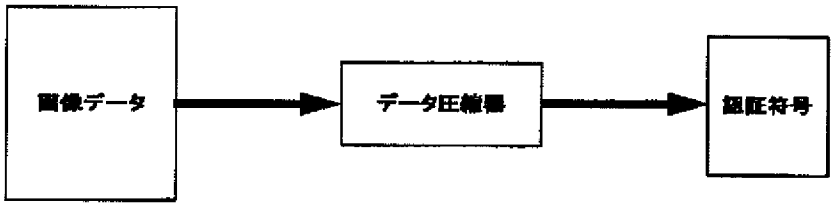
【符号の説明】

１　　記憶媒体

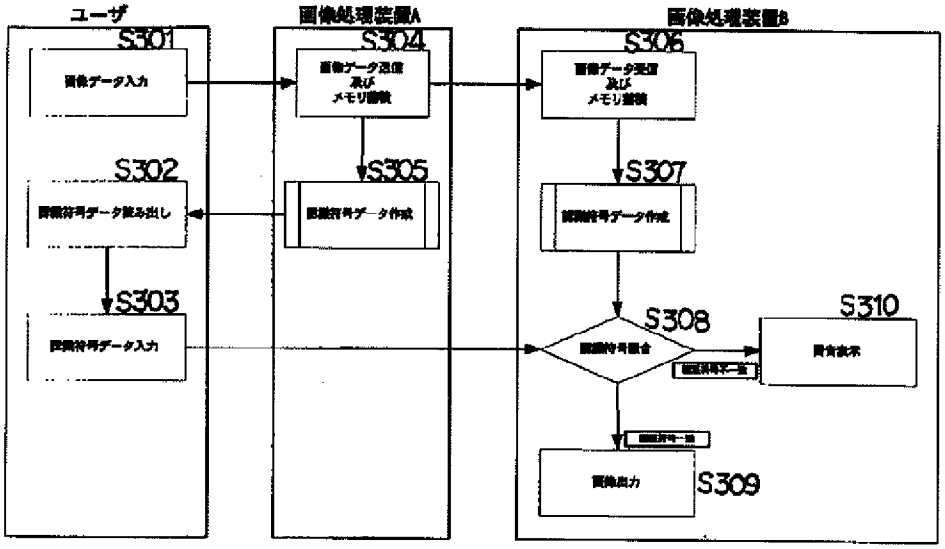
【図１】


出力
R
転送
出力
入力

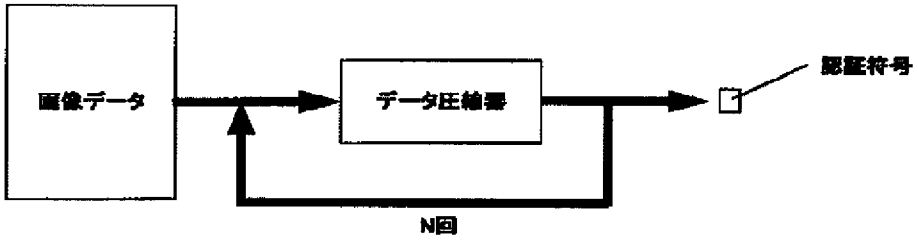
【図２】


画像データ
データ圧縮器
認証符号

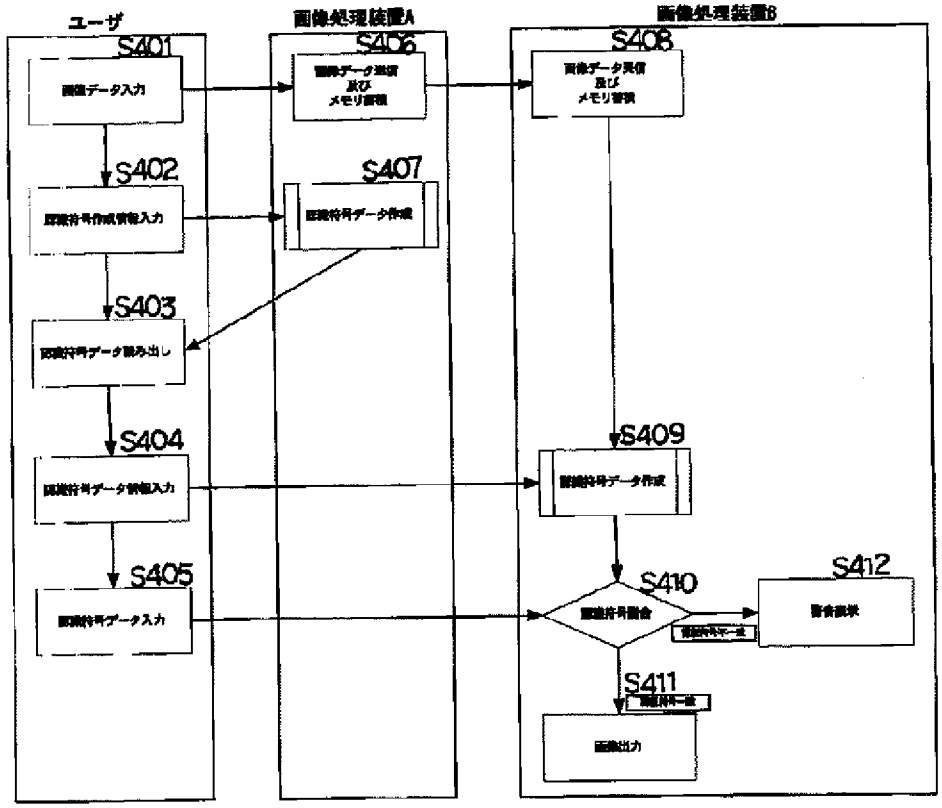
【図３】


ユーザ
画像処理装置A
画像処理装置B
S301
S302
S303
S304
S305
S306
S307
S308
S309
S310

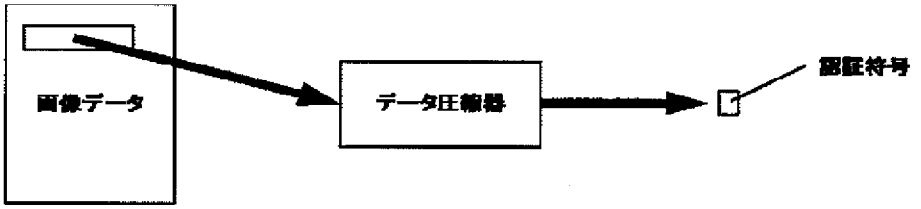
【図４】


画像データ
データ圧縮器
認証符号
N回

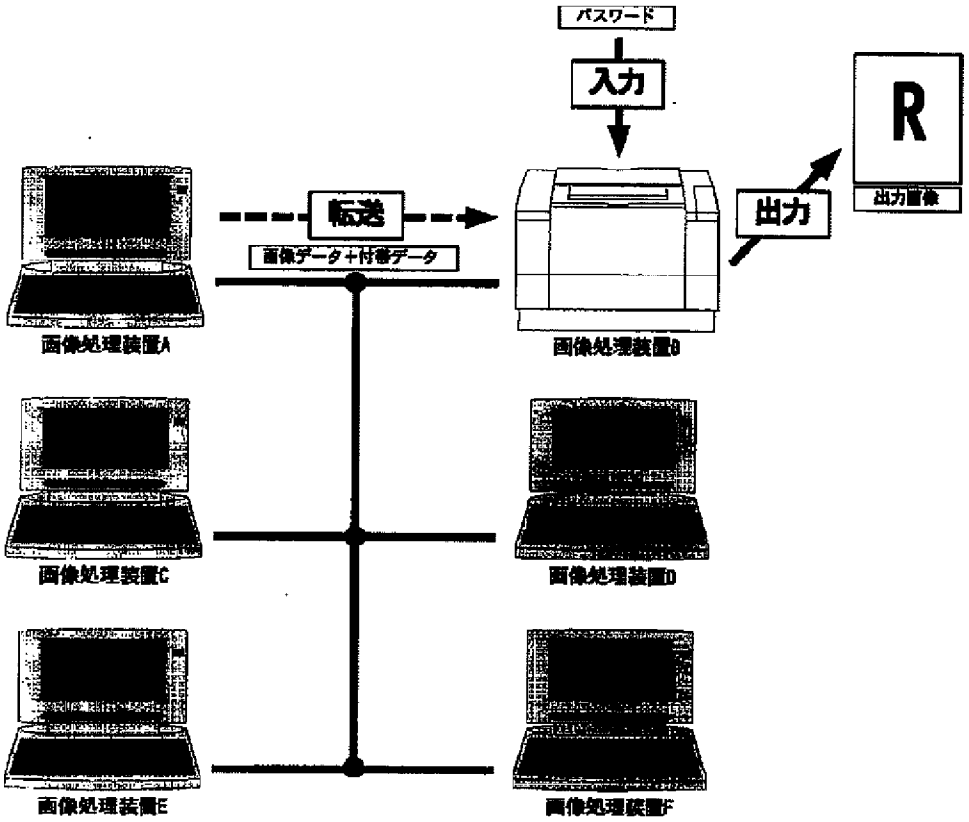
【図５】


ユーザ
画像処理装置A
画像処理装置B
S401
S402
S403
S404
S405
S406
S407
S408
S409
S410
S411
S412
画像出力

【図６】


画像データ
データ圧縮器
認証符号

【図７】


パスワード
入力
R
出力画像
転送
出力
画像データ＋付帯データ
画像処理装置A
画像処理装置B
画像処理装置C
画像処理装置D
画像処理装置E
画像処理装置F